

Pensamientos en voz alta

LA FIEBRE DEL BLOG

JAN
18

HowTo: VPN / IPSec / L2TP CON CERTIFICADO THAWTE O FNMT (III) CONFIGURACIÓN L2TPD

Category: [Posts](#)

La configuración de de L2TP radica en 3 ficheros:

```
/etc/l2tpd/l2tpd.conf # Parametros globales de la conexión  
/etc/l2tpd/options.l2tpd # Paramatros opcionales de configuración  
/etc/ppp/chap-secrets # Fichero de usuario y passwords
```

No comments

JAN
18

HowTo: VPN / IPSec / L2TP CON CERTIFICADO THAWTE O FNMT (II) CONFIGURACIÓN OPENSWAN

Category: [Posts](#)

Llegados a este punto decir que este ejemplo es para una distribución Debian etch, aunque está probado y funcionando también en ubuntu (LTS y gutsy) y OpenSUSE (10.x).

Instalaremos los siguientes paquetes y sus dependencias que necesitaremos:

```
# apt-get install openswan l2tpd xl2tpd ipsec-tools openssl
```

Y ahora la configuracion, que básicamene en OpenSWAN son estos 2 ficheros.

```
/etc/ipsec.conf : Este fichero configura IPSec y sus conexiones  
/etc/ipsec.secrets : Este otro fichero configura la autenticación IKE/IPSec
```

El resto de ficheros si no se le indica otra cosa en el fichero de configuración estan en:
`/etc/ipsec.d/`

Veamos en ejemplo de la configuración de `/etc/ipsec.conf`:

```
version 2.0
```



Google™

Buscar

☐ Web ☒ melic.es

October 2010

M	T	W	T	F	S	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

« Jan

VI MI VIDA PASANDO EN DIAPOSITIVAS

- > [Ainsa](#)
- > [Alquezar](#)
- > [Burriana-06](#)
- > [Calocen](#)
- > [Daniel](#)
- > [JYK](#)

```
config setup
interfaces=%defaultroute
klipsdebug=all
plutodebug=none
nat_traversal=yes
forwardcontrol=yes
virtual_private=%v4:10.0.0.0/8,%v4:172.16.0.0/12,%v4:192.168.0.0/16

conn %default
keyingtries=0
compress=yes
disablearrivalcheck=no
authby=rsasig
leftrsasigkey=%cert
left=1.1.1.1
leftnexthop=1.1.1.4
leftcert=mi.servidor.vpn.pem
rightrsasigkey=%cert

conn L2TP-CERT-WINXP-SP
type=transport
leftprotoport=17/1701
right=%any
rightprotoport=17/1701
pfs=no
auto=add

conn L2TP-CERT
type=transport
leftprotoport=0/1701
right=%any
rightprotoport=17/1701
pfs=no
auto=add
```

Así visto a lo bruto y por primera vez asusta un poco pero intentaré explicarlo brevemente ya que para ir a algo mas profundo los desarrolladores y curran unos buenos manuales y paginas man.

Básicamente el fichero consta de 2 partes, la primera *'config setup'* que es la configuración del servidor y luego todas las conexiones que tengamos definidas *'conn XXXXXX'*. Por simplificar lo que dice la configuración y no ir línea por línea explicando cada punto es que la autenticación va a ser por certificado: *authby=rsasig* y en la configuración por defecto definimos nuestro lado de la VPN (left) como:

```
left=1.1.1.1 # La ip WAN de mi servidor VPN
leftnexthop=1.1.1.4 # Gateway del servidor VPN
leftcert=mi.servidor.vpn.pem # Certificado de mi servidor VPN
```

La siguiente línea *rightrsasigkey=%cert* nos indica que la autenticación será por fichero de clave RSA. Ese que hemos creado antes llamado *certificado_FNMT.rsa* y que copiaremos al directorio */etc/ipsec.d/certs/*.

También necesitaremos crear nuestra clave pública y privada para nuestro servidor VPN. Podéis seguir una guía perfecta de como crear dicho certificado además de como crear diferentes VPN con OpenSWAN y muchísimo mejor explicado que yo, y eso que está en correctísimo inglés, [aquí](#)

Antes de pasar a explicar la configuración de L2TP quiero explicar que en las conexiones creadas en el fichero de configuración ipsec.conf de OpenSWAN hay 2

- > [Menorca](#)
- > [Piedrafita](#)
- > [Thailandia](#)
- > [Verano-09](#)

CATEGORIES

- > [Posts](#)

ARCHIVES

- > [January 2008](#)
- > [March 2006](#)
- > [December 2005](#)
- > [November 2005](#)

casi iguales : *L2TP-CERT-WNXP-SP* y *L2TP-CERT*. Son iguales excepto en la configuración del protocolo de transporte y es que el cliente l2tp de Microsoft no trata de la misma manera el protocolo IP dependiendo de la versión de S.O y del ServicePack que se tenga instalado.

Para versiones anteriores a WinXP-SP1 será la conexión L2TP-CERT y para versiones con WinXP-SP1 o superior será la L2TP-CERT-WNXP-SP.

No comments



HowTo: VPN / IPSec / L2TP con certificado Thawte o FNMT (I) CREACIÓN DE CERTIFICADO

Category: [Posts](#)

Escribo este post por 2 motivos muy diferentes, el primero porque tal y como sabe la gente que me conoce, suelo olvidar las cosas con mucha facilidad y el segundo por motivos meramente altruistas.

Recojo en estas líneas un pequeño HowTo de cómo crear un servidor Linux / IPSec / VPN / L2TP con certificado digital de la FNMT o thawte. Aunque bien podría ser con cualquier certificado digital creado por vosotros mismos.

Antes de nada para el que haya hecho su declaración de la renta por INET y posea su certificado digital de la FNMT es ese el que usaremos, para el que no tenga un certificado digital de la FNMT puede descargarse uno válido y gratuito de uso personal por una CA reconocida como es thawte en la siguiente dirección: <https://www.thawte.com/cgi/enroll/personal/step1.exe>.

Partimos de la base que tenemos el certificado exportado en formato .p12 o .pfx y copiado en nuestra máquina que hará de servidor VPN. Lo que vamos a hacer será desmontar el certificado en sus 2 partes, tal y como comenta en su blog [alguien](#) con quien comparto muchos genes, incluso más que con [la mosca del vinagre](#).

Desmontamos y sacamos el certificado del fichero exportado.

```
$ openssl pkcs12 -in certificado_FNMT.p12 -out certificado_FNMT.key -nocerts
```

La primera password que nos pide es la password que se le puso cuando exportamos el certificado y luego se nos pedirá que le pongamos una nueva password para proteger nuestro fichero *certificado_FNMT.key* que se creará a continuación.

Ahora extraeremos la clave privada de nuestro fichero *certificado_FNMT.key* introduciendo la password de uso del mismo

```
$ openssl rsa -in certificado_FNMT.key -out certificado_FNMT.rsa
```

Una vez hecho esto ya tenemos nuestra clave privada en el fichero *certificado_FNMT.rsa*

No comments



!!! I'M ALIVE !!!

Category: [Posts](#)

Si, ya se que hace tiempo que no escribo, y esto sólo lo leo yo, pero este post es para recordarme a mí mismo que tengo retomar esto cuando *Muchachito Bombo-Infierno* (AKA Daniel) y *La Mala Rodríguez* (AKA Desita) me permitan continuar...

1 comment



MIGRACIONES

Soy, como muchos otros, de los que piensan que las migraciones de plataformas han de ser lo menos traumáticas posibles para los usuarios finales que las usan. Mucho se ha escrito también de como se pueden hacer y también muchos que migran en una noche y al día siguiente los usuarios se encuentran con su flamante LINUX de escritorio en sus puestos de trabajo.

Así que dicho todo estos sabréis que antes de realizar la migración soy de la opinión de que al usuario hay que darle un tiempo para habituarse a sus nuevas aplicaciones (FireFox, OpenOffice, Thunderbird, etc...) y que mejor que éstas para empezar. Personalmente uso todas las anteriores y no, no uso Windows, perdón, si que lo uso, ¿que queréis ? en algún sitio he de jugar al Call of Duty 2.

Pero a lo que iba, la peor migración de todas (para mí) es la llamada de agujero negro. Sí, esa es la que cuando caes no puedes salir, y no es otra que Outlook y Exchange. Cuantos rompimientos de cabeza, pruebas con conectores y demás hasta que porfin lo encontré, y ha estado allí todo este tiempo y no es otra cosa que el fantástico servidor KOLAB.

En cuanto lo acabe cuelgo como montarlo....

No comments



Que mejor manera que de empezar con un post que mostrando el primer servidor WEB del mundo. El que usaba por 1989 Tim Berners-Lee. Una workstation de NeXT (un NeXTcube), que llevaba incorporada como extras una de las mejores cosas que describen lo que es un servidor, la pegatina de aviso con el siguiente texto.

“This machine is a server. DO NOT POWER IT DOWN!!”

Una copia original de la primera página web, creada por Berners-Lee, podeis encontrarla [aquí](#)

No comments

No he querido cambiar el texto por defecto de este primer post por 2 motivos, a saber:

- 1.- Por mi mas absoluta admiración a los creadores del proyecto ENQUIRE allá por 1989 y a su progenitor [Tim Berners-Lee](#) por haber regalado al mundo el [World Wide Web](#).
- 2.- Por que esto es un Blog (o bitácora), o lo que es lo mismo, un sitio donde cada uno expresa lo que siente, opina, motiva, etc...

Y es a este último punto donde quería yo llegar, por eso el título de este sencillo blog.

PENSAMIENTOS EN VOZ ALTA. Que mejor manera de definir lo que es este blog y el uso que se le va a dar.

[No comments](#)